**Gossip-6 LAYER4 Secure Communication Protocol**

1. Need secure communication:

* Establish shared AES256 key: Diffie Hellman key exchange,
* Need to trust the source (signature),
* Since there will be no CA, we need Proof of Work for the identity,
* We are already given an out-of-band public key sharing mechanism.

1. For Alice (client):

* Let handshake message such that for some pre-determined and Scrypt hash function with configuration ,
* Sign the digest with as ,
* Add the signature to the message as and send to Bob (server).

1. For Bob (server):

* Upon receiving , get the fields of the message as ,
* Check validity first as , if not valid then discard connection,
* From , get the fields ,
* Make sure is a known and trusted public key**\***,
* Verify signature as , if not valid then discard connection,
* Let handshake message such that for some pre-determined and Scrypt hash function with configuration ,
* Sign the digest with as ,
* Add the signature to the message as and send to Alice (client).

1. For Alice again (client):

* Upon receiving , get the fields of the message as ,
* Check validity first as , if not valid then discard connection,
* From , get the fields ,
* Make sure is a known and trusted public key**\***,
* Verify signature as , if not valid then discard connection.

1. Now that both Alice and Bob have and , they can both calculate the shared secret as . After 1 round trip, the secure communication has been established. Each message following the handshakes will be encrypted with the .